ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

ICO Call for Views

Code of Practice for the use of personal information in political campaigns

ISACA Response

This response is being submitted on behalf of ISACA and the CMMI Institute. By way of introduction, ISACA is a global non-profit association helping individuals and enterprises achieve the positive potential of technology. ISACA help individuals to lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. ISACA also plays a leading role in the UK by providing accreditation for IT professionals, both in the cyber security and IT Audit sectors, most notably through our COBIT 5 framework.

The CMMI Institute is the organisation behind the Capability Maturity Model Integration (CMMI), the globally adopted capability improvement framework that guides organisations in high-performance operations, and the Institute's Cybermaturity Platform, which provides a risk-based approach to measuring and managing security risks in enterprise operations, tailored to the context of the business and its strategy. This CMMI solution provides the tools and support for organisations to benchmark their capabilities and build maturity by comparing their operations to best practices and identifying performance gaps.

This response pertains to some of the issues that require addressing to assure integrity in electoral process, and the principles the ICO should seek to address in the code of practice for use of personal information in political campaigns.

Election Data Integrity

Elections are crucial to the functioning of representative democracy and election processes being compromised can delegitimise a whole political system. Elections have become an increasingly frequent target in the modern digital era and have been subject to cyber-attacks – most likely combined with information operations and other hybrid threats. Given this threat, this must be reflected in planning assumptions and risk management.

Although allegations of nation-state interference in the US election process has commanded much of the media attention, protecting the overall data integrity of elections is a much more encompassing issue than any attempt by a nation-state to influence a particular election cycle or

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

campaign. Working to enhance the reliability of the information systems and technology that assures data integrity in the electoral process will be an ongoing challenge requiring attention and support from leaders at all levels of Government.

Encouragingly, this challenge is clearly on the radar of the ICO, the European Commission and elected officials in the U.S. In the U.S., a recently formed Task Force on Election Security, composed of members of the Homeland Security Committee and House Administration Committee, allowed for members from both committees to interact with election stakeholders, as well as cybersecurity and election infrastructure experts, to analyse the effectiveness of the US election system. The task force produced a final report and future recommendations, with the goal of maintaining free, fair and secure elections. Likewise, a report led by the Estonian Information System Authority has been published following the creation of a cooperation group established by the NIS Directive. The report found that coordinated cyber-attack could be so severe as to hamper the democratic process and obstruct the European Parliament from convening after the elections.

Given the high stakes involved and the growing complexities of the threat landscape, election systems require more dedicated resources to ensure the appropriate people, processes and technology are in place to stave off threats to not only election data integrity but also threats to public belief in institutions. Endemic disinformation within political campaigns, addressed at delegitimising democratic institutions, represents a significant threat to the future of democracy.

Whilst misuse of data in election campaigns have been heavily investigated and scruitinsed, apparent attempts to use similar tactics of spreading propaganda and disinformation on social media platforms to corrode the legitimacy of structures such as the judicial system have drawn much less scrutiny from policymakers. Attempts to baselessly discredit these structures should be examined in depth by policy makers and action taken to ensure disinformation campaigns do not harm the legitimacy of democratic and established institutions.

Government funding allowing for the training of election officials and poll workers about cyber risks would be another worthwhile investment. Further, since elections are generally run at the local level, Government agencies need to increase coordination to allow for real-time notifications of security breaches and threats.

Additionally, Government's should conduct post-election audits in order to ensure the election was not compromised, as well as identify and limit future risks. The implementation of post-

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

election audits is an immediate step the Government can take to limit future vulnerabilities while also strengthening public trust in the process – an important consideration that should not be overlooked.

One intriguing longer-term solution for election data integrity is the deployment of blockchain technology. Blockchain is now being embraced by many different sectors and agencies, and was recently used in West Virginia for absentee voting leading up to the U.S. midterms. Blockchain has the ability to secure a permanent record that is timestamped and signed and can therefore not be altered in any way. Developing this cyber-attack resilient database could prove to be a critical step toward mitigating any potential manipulation or voting fraud.

While audit, governance, risk and information/cyber security professionals are charged with many important responsibilities, helping to solidify the data integrity of elections is among the most vital. Trustworthy elections are an indispensable component of free societies. Losing trust in the outcomes of elections would lead to a level of discord that would have a profoundly destabilising impact. The events of the past few years have reinforced that protecting the integrity of the electoral system in this new era will require a significant investment in attention and resources.

Guiding principles

ISACA believe that the ICO should seek to use the following guiding principles to guide its Code of Practice around Political Campaigns:

The networks and systems utilised for political campaigning should be encouraged to establish the necessary levels of cyber maturity. This pertains to both Government systems and the private sector in the domains of political advertising. A maturity approach to cyber resilience would allow for increased transparency, increased understanding of risk areas and what is required to address these issues; and this would enable the relevant organisations to continue with their day to day operations with a lower attack threat level. The Government and ICO could consider establishing the need for political parties, third sector groups and social media companies to establish a cyber maturity approach to address cyber risks.

Given the volume, magnitude and speed of technological changes and the transformations to the growing complexity of data management, ISACA would also advocate for independent audits to be conducted after every election. Good IT audit hygiene must lie at the center of protecting the integrity of data in elections. By conducting regular post-election audits, greater understanding

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

of the threat landscape can be established and as such practice can be adjusted accordingly. It is only by moving forward measures to protect the integrity of elections that we can ensure that risks have been addressed and personal data and election outcomes can be protected.

The ICO in accordance with Government departments may wish to examine the potential uses of blockchain in creating a cyber-attack resilient database. Use of this technology would ensure that personal information held by all parties would be protected to the highest possible standards. This is critical to maintaining the trust and integrity in the election process.

The Government might wish to consider the need for action to be taken to prevent misinformation campaigns aimed at delegitimising democratic institutions. Potential actions include, a requirement for social media companies to spread myth debunking in conjunction with flagging unverified stories. The Government could also consider extending libel law to recognise the severity of attempting to undermine democracy through fake news.

If these principles are addressed in the ICO's Code of Practice, it will mark an important step in addressing the integrity of data in elections and political campaigns.

For more information please contact: